

KASPERSKY LAB

**SECURE
YOUR
CYBERSPACE**

www.kaspersky.com



**Kaspersky Anti-Virus® 5.0
for Windows Workstations**

USER GUIDE

KASPERSKY ANTI-VIRUS® 5.0
FOR WINDOWS WORKSTATIONS

User Guide

© Kaspersky Lab Ltd.
<http://www.kaspersky.com>

Revision date: March, 2005

Contents

CHAPTER 1. COMPUTER VIRUSES AND MALWARE	5
CHAPTER 2. IF YOUR COMPUTER IS INFECTED... ..	7
2.1. Symptoms of infection	7
2.2. What to do if you have any of these symptoms	8
2.3. If viruses are found during a scan	9
2.4. If nothing helps.....	10
2.5. After you eradicate the infection.....	10
CHAPTER 3. KASPERSKY ANTI-VIRUS® FOR WINDOWS WORKSTATIONS	11
3.1. Product package.....	12
3.2. Services for registered users	13
3.3. Adopted conventions.....	13
CHAPTER 4. PROGRAM INTERFACE	15
4.1. System tray icon	15
4.2. Right-click menu	15
4.3. Main program window: general structure	16
4.3.1. <i>Protection</i> tab	18
4.3.2. <i>Support</i> tab	19
4.4. Scanning process window	20
4.5. Help system	21
CHAPTER 5. WORKING WITH THE PROGRAM	22
5.1. Updates for the anti-virus database and application modules	22
5.1.1. Choice of time for updating.....	22
5.1.2. Update procedure	23
5.2. How to prevent a virus infection	24
5.2.1. When do I need to scan my computer and particular objects?	25
5.2.2. Full scan	26
5.2.3. On-demand scans of selected files or folders	26
5.2.4. Scan of archives	29
5.2.5. Treating suspended objects	30

5.2.6. How to scan a CD or a floppy disk	32
5.3. Real-time protection	33
5.4. Additional features	34
5.4.1. Quarantine and Backup storage	34
5.4.1.1. Work with Quarantine storage	34
5.4.1.2. Work with Backup storage	36
5.4.2. Work with reports	37
APPENDIX A. FREQUENTLY ASKED QUESTIONS	41
APPENDIX B. CONTACTING TECHNICAL SUPPORT SERVICE	46
APPENDIX C. GLOSSARY	48
APPENDIX D. KASPERSKY LAB	52
D.1. Other Kaspersky Lab Products	53
D.2. Contact Us	57
APPENDIX E. INDEX	58
APPENDIX F. LICENSE AGREEMENT	59

CHAPTER 1. COMPUTER VIRUSES AND MALWARE

The risks of computer virus infection and data damage or theft through other malicious software has grown as the number of computer users increases, together with the number of opportunities for data exchange between them via e-mail and the Internet.

It would be useful to learn about the types of malware and how they function in order to understand the threats that they pose to your data.

The following classes of malware can be defined according to their specific manifestations:

- **Worms** – malware belonging to this category copies itself to network resources. The name of this class comes from the ability of worms to “crawl” from one computer to another through networks, e-mail and other informational channels. This feature enables worms to spread extremely quickly.

They penetrate computer memory, calculate network addresses of other computers and send copies of themselves to those addresses. Apart from network addresses, they frequently use the data from e-mail client address books. Programs of this class may sometimes have work files on system disks, but they might not use any resources on a computer at all (except for RAM).

- **Viruses** – programs that infect other programs by embedding their own code into the latter in order to gain control when infected files are launched. This simplified definition lets us identify the main action that a virus performs – *infection*. Viruses spread somewhat slower than worms.
- **Trojans** – programs that perform actions which the user has not authorized; for example, depending upon certain conditions, they may destroy the information recorded on disks, cause the system to “hang”, steal confidential data, etc. Programs belonging to this class are not viruses in the traditional understanding of the term; Trojans cannot penetrate target computers independently and therefore they are passed off by intruders as “useful” software.
- Damage caused by Trojan software may exceed the losses from traditional virus attacks by tenfold, since the consequences of viruses may be minimized using an adequate backup system.

In recent times, worms have become the most wide-spread type of malware corrupting computer data. Then viruses and Trojans follow, judging by the

frequency of their occurrence. Some malicious programs combine the properties of two or even three of the classes mentioned above.

The following types of potentially dangerous software also became widely spread:

- **AdWare** – software code for advertisement demonstration added into a program without informing the users about that. As a rule, adware is built into free software. The advertisement appears within the program interface. Such programs frequently collect and transmit to their developers some personal information about users, change various browser parameters (home and search pages, security levels, etc.), generating additional traffic, which users do not control. All of the above may cause violations of the security policy or even direct financial losses.
- **Riskware** – software that does not have any harmful functions but may be employed by intruders as an auxiliary component for malware programs because of the security breaches and errors it contains. The category includes, for example, remote administration software, IRC clients, FTP servers, various utilities used to terminate processes or hide their activity.
- **SpyWare** – software designed for unauthorized access to user data, tracking of actions performed on a computer, collection of information about hard drive contents. Such tools allow an intruder to gather data or even control a computer from outside. Spyware is usually distributed with free software and deploy on a computer imperceptibly for its user. Spyware category includes software tracking keyboard input, password cracking tools, programs for collection of confidential data (e. g., credit card numbers).
- **PornWare** – programs that establish charged modem connections to various Internet sites, mostly with adult content.
- **Hack Tools** – software employed by intruders for their own purposes to gain access to your computer. The category includes various illegal scanners of vulnerabilities, password cracking tools, other types of software for breaking into network resources or intrusion into an attacked system.

E-mail and the Internet act as the main sources for spreading virus infections and malware, although infection may be caused by a floppy disk or a CD. This situation reflects a shift of emphasis in anti-virus protection from simple regular scanning of computers for virus presence to a more complex process of real-time computer protection from a probable infection.

CHAPTER 2. IF YOUR COMPUTER IS INFECTED...

Sometimes it is not always apparent, even to a knowledgeable user, that a computer is infected with a virus or a Trojan, because these programs mask their presence among useful files. This chapter describes in detail how to recognize the infection, restore data after a virus attack, and prevent malicious programs from getting onto your computer.

2.1. Symptoms of infection

There are a number of common symptoms which indicate that your computer has been infected. If you have noticed one of the following symptoms, a virus has probably infected your computer:

- Unexpected messages or images are suddenly displayed.
- Unusual sounds or music is played at random times.
- Your CD-ROM drawer mysteriously opens and closes.
- Programs are suddenly launched on your computer.
- If Kaspersky Anti-Hacker is installed on your computer, you receive notifications about attempts of some programs to connect to the Internet without your permission.

In addition, there are other typical symptoms indicating that your computer has been infected via e-mail:

- You receive notifications that the message you sent contained a virus but the anti-virus program of the recipient declined your message, whereas in reality, you did not send this message or are sure that the message was free of viruses.
- Your contacts receive messages from your address that you did not send.
- Your mailbox contains many messages without the sender's address and the header.

Note that these problems are not necessarily symptoms of virus-like activities. They can have other causes. For example, infected messages from your address can be sent from another computer.

You might have noticed the following indirect symptoms point to a virus infection on your computer:

- Your computer freezes frequently or displays error messages.
- Your computer slows down when programs are launched.
- Your attempts to boot up the operating system fail.
- Files and directories suddenly go missing or their content changes.
- Your hard disk is accessed too often (the light below the power button blinks).
- Microsoft Internet Explorer "hangs" or behaves erroneously (for example, you cannot close a program window).
- Your computer cannot boot from the hard drive (an error message is displayed).

Note that 90% of such cases indicate problems with your hardware or software. However, the remaining 10% indicate a possible infection of your computer. If you experience any of the above symptoms, we recommend that you contact your system administrator and conduct a comprehensive virus scan of your computer.

2.2. What to do if you have any of these symptoms



If you have noticed that your computer is behaving "suspiciously":

1. Don't panic! This golden rule prevents you from unnecessary stress and helps you save important data stored on your computer.
2. If you cannot boot from the hard drive (your computer gives you an error message when you are starting the system), try to start the system in safe mode or from the Windows boot disk that you created during installation of the operating system on your computer.
3. Before taking any actions, back up all critical data on an external storage device (floppy disk, CD, flash card, etc.).
4. Install Kaspersky Anti-Virus, if you have not yet installed it.

5. Retrieve the latest updates for your anti-virus database. If possible, retrieve the updates using an uninfected computer. This is quite important, because if you are connected to the Internet, a virus can send important information to the perpetrators or try to send itself to everyone in your address book. Therefore, if you suspect that your computer is infected, immediately disconnect it from the Internet. However, if there is no other way of retrieving the updates, you can take the risk and download updates before disconnecting.
6. Disconnect your computer from the Internet.
7. If your computer is connected to a local network, disconnect it.
8. Launch a full scan (see section 5.2.2 on p. 26).
9. Inform your system administrator about suspicious symptoms in computer operation.

2.3. If viruses are found during a scan

If viruses are found during a scan, Kaspersky Anti-Virus will automatically disinfect them and recover the data on your computer according to the settings.

Note that in 99% of cases, computers suffer from e-mail worms, Trojan programs, or viruses (see Chapter 1 on p. 5 about malicious programs). In virtually all cases, lost data can be successfully restored.



To remove viruses and recover damaged data:

1. Do not interrupt the operation of Kaspersky Anti-Virus. During a full scan, the program will disinfect infected files, move suspicious files to a quarantine folder, and delete mail worms and Trojans. Before curing upon scan completion Kaspersky Anti-Virus will display all the suspicious files, viruses, e-mail worms, and Trojans that it has detected. Also you can find the names of any virus resident on your computer in the report (see section 5.4.2 on p. 37).
2. In some cases, you might need a special recovery utility to restore corrupted data. Connect to the Internet and read the information at the Kaspersky Lab website (www.kaspersky.com) about a virus, a Trojan horse, or a worm that has infected your computer. Download the special utility for data recovery if such a program exists for a specific virus. For example, to recover data infected with the **Klez** virus, download and run the *clrav.com* program.

3. Read the information about your situation on the website carefully. You will probably have to take additional measures.
4. If viruses (for example, **Nimda**, **Klez**, or **Badtrans**) have penetrated your computer by exploiting Microsoft Outlook Express vulnerabilities, they can reactivate even after Kaspersky Anti-Virus cleans the system, for example, when you are reading previously infected messages. Therefore, check if the protection mode that scans e-mail database is enabled (for more information, please contact your system administrator) and install the latest security patches for Microsoft Outlook to ensure its safe future operation.

Unfortunately, some viruses cannot be totally removed from infected objects. Some of them destroy information on your computer during infection.

2.4. If nothing helps...

If the symptoms described above persist even after you have scanned your computer, hardware, and software, and have checked your hard drive using Windows utilities, please feel free to send a letter with a full description of your problem to the Technical Support Service of Kaspersky Lab.

If you are sure that some files are Trojan programs or are infected, send these files to Kaspersky Lab for expert analysis.



For details of how to send messages and files to Kaspersky Lab, see Appendix B on p. 46.

2.5. After you eradicate the infection

After you get rid of the infection, scan all disks and floppy disks that may be infected with a virus.

Make sure that you have the latest version of Kaspersky Anti-Virus installed on your computer and you use the latest anti-virus database and the default settings recommended by the Kaspersky Lab experts (for more information about Kaspersky Anti-Virus settings, please contact your system administrator).

Read carefully **How to prevent a virus infection** section (see section 5.2 on p. 24) and pay attention to the main security rules that will help you to prevent future virus infections.

CHAPTER 3. KASPERSKY ANTI-VIRUS® FOR WINDOWS WORKSTATIONS

Kaspersky Anti-Virus® for Windows Workstations (also referred in this user guide to as Kaspersky Anti-Virus) is designed to protect workstations from the viruses and malware.

The following features have been implemented in the application:

- *Real-time protection of file system against malicious code in the monitoring mode:* interception and analysis of attempts to access the computer file system and network directories; disinfection or deletion of infected objects or isolation of suspicious objects for further analysis.
- *Scan for and neutralization of malicious code on user's or administrator's request:* detection and analysis of infected or suspicious objects in the defined scanning areas; removal of infected and isolation of suspicious objects for further analysis.
- *Checking potentially dangerous software:* analysis of programs started in the user's computer, downloaded from the internet or located on the hard drive or removable media. When potentially dangerous software is detected, the application (depending on the settings) will either allow or block its execution or remove this software from the user's computer.
- *E-mail scanning in the monitoring mode:* analysis of requests for e-mail sending or receiving. The anti-virus prevents e-mail messages containing malicious code from penetrating the user's mailbox or from sending suspicious or infected objects to other addresses. The anti-virus scans all incoming and outgoing Microsoft Outlook e-mail messages; it also scans incoming and outgoing e-mail messages of any mail clients that use SMTP and POP3 protocols.
- *Constant protection of office applications using VBA macros:* analysis of macro commands prior to their execution and prevention of potentially dangerous macro commands being executed.
- *Constant protection against execution of dangerous VBScript and JavaScript scripts:* scanning of script code prior to its execution by the OS script processing engine; blocking execution of dangerous scripts.
- *Quarantine of suspicious objects:* storage of discovered suspicious objects in a quarantine directory; on-demand dispatch of them to Kaspersky

Lab for further research; restoration of objects from the quarantine at administrator's or user's request.

- *Creation of copies in backup storage for infected objects prior to their disinfection or removal* in order to allow on-demand restoration of an object if the latter contains valuable data.
- *Updates for the anti-virus database and software modules* included in the Anti-Virus package from the Kaspersky Lab update servers; creation of backup copies for all files being updated if the last update needs to be rolled back; addition of received updates to a special directory for further distribution in order to reduce internet traffic.



Please keep in mind that new viruses emerge every day in the world. Therefore, it is recommended that you enable the automatic updates feature.

3.1. Product package

You can purchase the software from our distributors (retail box), or from one of our web shops (for example, www.kaspersky.com, **E-Store** section).

If you purchase a box product, the software bundle includes:

- sealed envelope with an installation CD containing software files;
- user's manual;
- license key included in the distribution package or recorded on a special floppy disk;
- license agreement.



Please read the license agreement carefully before opening the CD envelope.

If you purchase our product from an e-shop, or you copy it from the Kaspersky Lab site, the copy also contains this manual. Your license key is either included in the installation file or sent to you by e-mail after payment.

The license agreement constitutes a legal agreement between you and Kaspersky Lab containing the terms and conditions subject to which you may use the purchased software.



Please read the license agreement carefully!

If you do not agree to the terms of the license agreement, you may return the box with Kaspersky Anti-Virus to the distributor, where you have purchased it; you

will be refunded the amount you have paid for subscription, provided the CD envelope remains sealed.

Opening the sealed envelope of the installation CD or installing the product to a computer entails your acceptance of all the terms and conditions of the license agreement.

3.2. Services for registered users

Kaspersky Lab offers its legal users a broad range of services maximizing the efficiency of Kaspersky Anti-Virus use.

By purchasing a subscription, you become a registered software user entitled to the following services throughout the period of subscription validity:



- upgrades for the software;
- consultations regarding issues pertaining to installation, setup, and use of this software available over the telephone or e-mail;
- notifications about availability of new software products from the Kaspersky Lab and new viruses emerging in the world (that service is provided to users who have subscribed for e-mail newsletter from the Kaspersky Lab).





No consulting is offered for issues pertaining to operating systems functionality or use or operation of various technologies.

3.3. Adopted conventions

The text in this document uses various styles depending upon its purpose. The table below lists adopted conventions used in the text.

Style	Purpose
Bold face	Menu titles, menu items, window titles, parts of dialog boxes, etc.
 Note.	Additional information or notes
 Attention!	Information that should be given special attention



Style	Purpose
 <i>In order to perform the action,</i> 1. Step 1. 2. ...	Procedure description for user's steps and possible actions
 Task, example	Statement of a problem, example for using the software features





CHAPTER 4. PROGRAM INTERFACE

Kaspersky Anti-Virus has a simple and easy-to-use interface. This chapter is devoted to detailed description of its main components – the system tray icon, right-click menu, main window, and some service windows.

4.1. System tray icon

After the application has been launched, its icon appears in the system tray. The icon appearance depends on the status of anti-virus protection, demonstrating whether real-time protection is enabled or on-demand scanning has been started.


If the real-time protection is on, the icon will be active (red) , if it is off – the icon will be inactivated (gray) .

The icon will blink in the system tray  when full system scanning or scanning of an individual file, disk or analysis of some object in real-time mode is taking place. Scanning of incoming e-mail is indicated by the , and the  icon appears when errors occur when launching of any real-time protection tasks. The program changes its tray icon to  while downloading updates to the anti-virus databases and application modules.

If an event of some importance in terms of anti-virus protection occurs, an informational message box appears for a while over the icon and displays recommendation from the experts of Kaspersky Lab (this feature is not available in Windows98/NT).

4.2. Right-click menu

If you click the application icon in the system tray using the right mouse button, you will see a menu (see Figure 1) consisting of the following items:

- **Open Kaspersky Anti-Virus** – opens the **Protection** tab of the main program window. You can achieve the same result by double-clicking the program icon  in the system tray.

- **Scan My Computer for viruses** – launches complete computer scan for viruses in accordance with the defined level of protection.
- **Update the anti-virus database** – launches download of updates for the anti-virus database.
- **Running tasks** – this item appears in the right-click menu as soon as the Anti-Virus starts any scheduled tasks. Selection of that item brings up a submenu containing a list of all scheduled tasks running at the moment. Select a task from the list (please see Figure 4) in order to see the details of its activity.
- **About the application** – displays a help window with information about Kaspersky Anti-Virus for Windows Workstations.
- **Switch to user mode/ Switch to administrator mode** (only under MS Windows 98/ME) – switches respectively between a user interface and the extended administrator interface. Selection of the **Switch to administrator mode** option brings up a dialog box with a prompt to enter the password of the anti-virus security administrator.



Figure 1. Right-click menu

4.3. Main program window: general structure

The main window of Kaspersky Anti-Virus is designed for implementing all application's features, which gives your computer complete anti-virus protection. Here you can:

- start the anti-virus protection tasks;
- download updates for the anti-virus database;
- work with objects that have been quarantined or copied to the backup storage;
- work with report logs, etc.

All parameters of anti-virus protection, necessary information, and tasks are grouped in the following tabs of the main window:

- **Protection** – anti-virus protection status and tasks. The tab represents the main functionality while working with the application.
- **Support** – information required in case of problems or a need to address Kaspersky Lab for assistance.

Each tab is subdivided into two parts:

- **Task list** is the left frame of the tab containing the tasks which actually implement the anti-virus protection. The task list depends on tab purpose. The **Protection** tab, for example, contains tasks for complete scans of your computer for viruses.
- **Anti-virus protection status** is represented in the right frame of the tab including the information about current status of anti-virus protection for your computer (real-time protection, full system scans, and the anti-virus database). The **Protection** tab, for example, indicates the status of anti-virus protection.

There are three states for anti-virus protection status. They are indicated by the following icons:



Critical anti-virus protection status. This means that real-time protection is disabled, some of the tasks (scanning and/or updating) have not been performed for a long time, or the settings do not provide an adequate level of anti-virus protection for your computer; it also notifies the user of errors that occur while running an Anti-Virus task.



Anti-virus protection level is different from the recommended one. This status is reached when user-defined anti-virus protection settings do not correspond to the settings recommended by experts at Kaspersky Lab. It also indicates that a certain anti-virus protection task has to be performed.



Recommended level of anti-virus protection. The status means complete conformity of protection and anti-virus security settings to the recommendations of Kaspersky Lab experts.

Each of the above statuses is supplemented by comments and recommendations. Thus, for example, when the anti-virus protection level is different from the recommended one, to the program will propose that you return to recommended settings, since they provide for the optimal level of anti-virus protection.

4.3.1. *Protection* tab

The **Protection** tab (see Figure 2) is designed for running tasks which provide full system scanning as well as scanning individual disks, folders, or files. Here you can also launch update downloads for the anti-virus database. The tasks may be started by corresponding hyperlinks in the left part of the tab.

The left part of the tab also contains links to quarantine and backup storage and program reports:

- [Quarantine](#) – open suspicious objects' storage window.
- [Backup](#) – open infected objects' backup storage window.
- [Reports](#) – open reports log.

In the right part of the tab you can review the *current status of real-time protection, full system scanning, and anti-virus database*. Kaspersky Anti-Virus *recommendations* represent an essential attribute of critical or medium status levels of anti-virus protection.

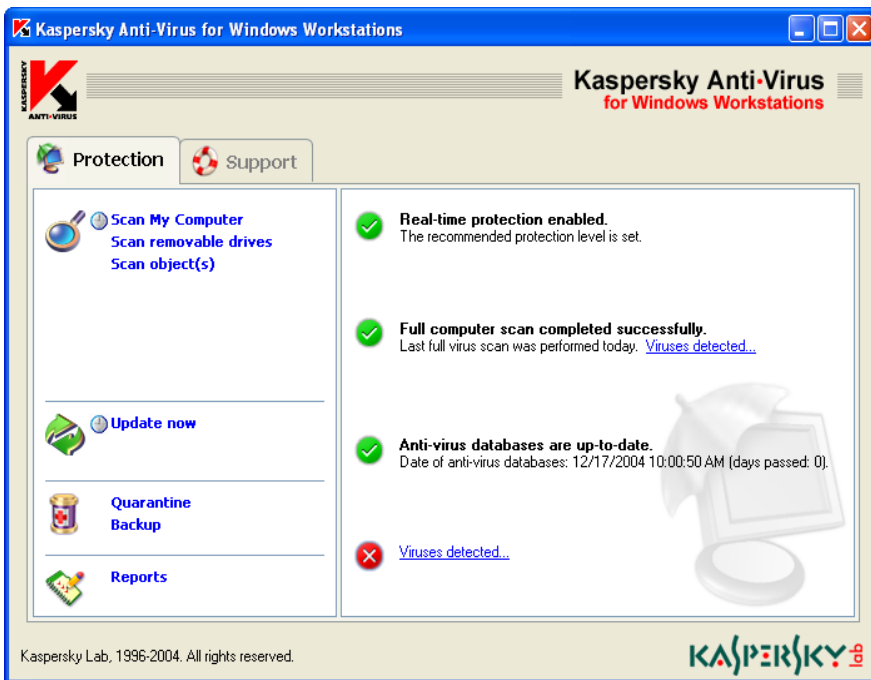


Figure 2. **Protection** tab

The right panel of the tab under status indicators of anti-virus protection displays some general information about the total number of objects scanned and viruses detected since installation of Kaspersky Anti-Virus.

General information about the number of scanned objects and viruses detected after Kaspersky Anti-Virus was started is presented in the right part of the tab under the area containing the anti-virus status information.

The information is replaced with a [Viruses detected...](#) hyperlink if a scheduled scanning task discovers infected or suspicious objects. Clicking the hyperlink will take you to the list of tasks which have assigned some objects for subsequent treatment.

4.3.2. **Support tab**

Using the **Support** tab (see Figure 3), you can access information about the Technical Support Service, which you should call in case of problems pertaining to Anti-Virus operation or situations which you cannot handle by yourself. It contains information about the program, your license key, and the operating system installed on your computer. All that information is displayed in the right part of the tab.

The left frame contains the following hyperlinks:

- [Send question to technical support](#) – send a question concerned with Anti-Virus operation to Technical Support.
- [Send file for analysis](#) – send an e-mail with a suspicious object to Kaspersky Lab for analysis.
- [Help us to make this product better!](#) – send a suggestion to the Technical Support Service through the automated system of feedback processing. Clicking the hyperlink opens a feedback collection form on the web site of Kaspersky Lab.

The left part of any tab in the main window of Kaspersky Anti-Virus contains links to help information:

- [Help](#) – general help for the software.
- [How to...](#) – help system for task performance and resolving emerging issues.
- [Virus Encyclopedia](#) – a link to www.viruslist.com, which contains a detailed description of all currently existing malware.
- [Kaspersky Lab's Website](#) – a link to the Kaspersky Lab web site.

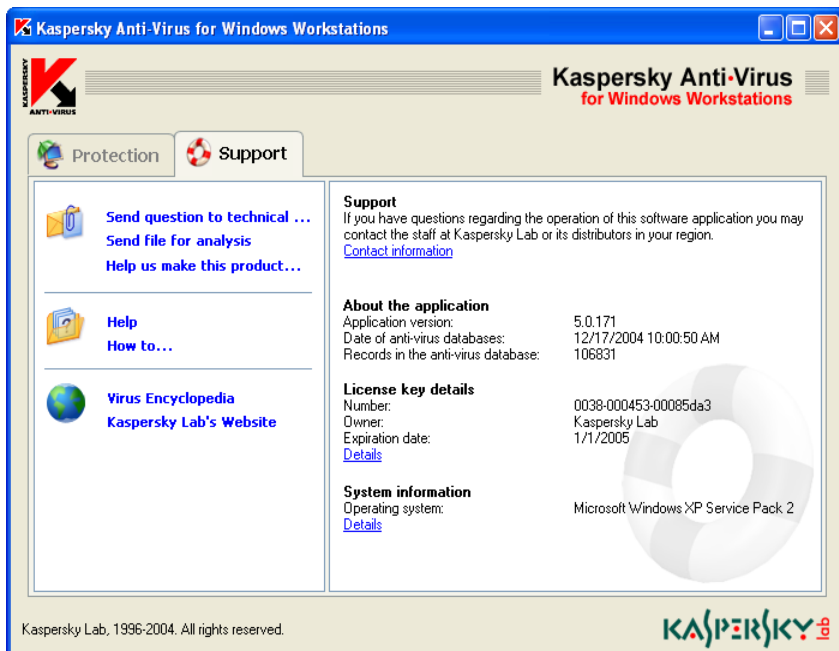


Figure 3. Support tab

4.4. Scanning process window

When a computer scan or scan of its individual objects (disks, folders, files) is launched, the scanning process window appears on the screen (see Figure 4).

The window consists of two parts:

- The upper part demonstrates the scanning progress indicator, the time of process was begun, estimated completion time, and the name of the file being scanned at the moment.
- The lower part consists of three tabs: a **Statistics** tab with statistical results of the scan, a **Report** tab containing the report on events which have occurred during the scanning procedure, and a **Settings** tab with a list of settings used for the recent or current scan.

The [View quarantine](#) hyperlink takes the user to the quarantine storage window (see section 5.4.1.1 on p. 34).

Use the [Export report to file](#) hyperlink to save the report as a text document. Clicking the link opens a standard browsing window, where you should enter the

destination file name, select the target directory on disk and click the **Save** button.

If the application detects infected or suspicious objects during scanning for which delayed processing has been enabled, it will add the [Detected viruses](#) hyperlink, by pressing which you can open a management window for the infected objects that will be processed later (see section 5.2.5 on p. 30).

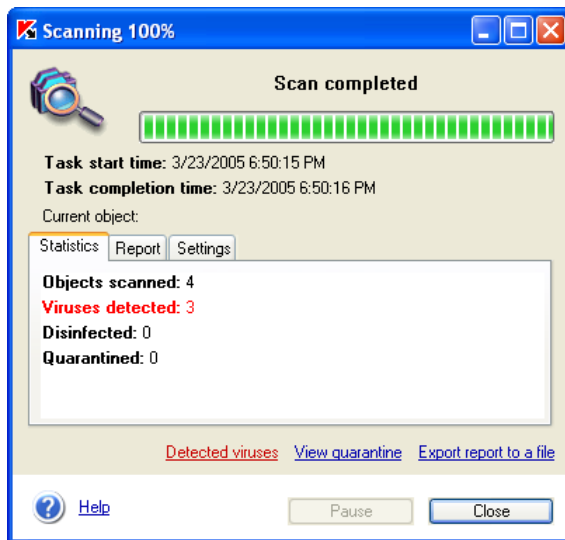


Figure 4. Scanning process window

4.5. Help system

Comprehensive program reference information is available from the **Support** tab of the main application window by simply following the [Help](#) link in the left section of the tab.

When you need to know how to perform a particular task, follow the [How to...](#) link in the main Kaspersky Anti-Virus for Windows Workstations window. [How to...](#) contains a detailed description of the key anti-virus protection tasks performed by Kaspersky Anti-Virus for Windows Workstations as well as an FAQ.

If you have a question on a particular dialog box, press the **<F1>** key or click [Help](#) in the bottom left-hand corner of the dialog box.

CHAPTER 5. WORKING WITH THE PROGRAM

5.1. Updates for the anti-virus database and application modules

Efficient operation of Kaspersky Anti-Virus depends on current information to reliably protect your computer from newly discovered threats. Kaspersky Lab makes this information available to its customers through a regularly updated anti-virus database.



Downloading updates for the anti-virus database ensures constant anti-virus protection of your computer. Hundreds of new viruses appear daily, and every day Kaspersky Anti-Virus experts update our anti-virus database with the latest information about these new threats. We recommend that you update your anti-virus database every hour.

To download the updates, Kaspersky Anti-Virus connects to one of the Kaspersky Lab update servers, accessible via the Internet, or to a local update server.

Updates can be downloaded automatically by using a recommended schedule created at when the application is installed or by using a schedule customized by administrator. The program downloads and applies the updated database while connected to the Internet. Kaspersky Anti-Virus copies the updates from remote update servers and installs the necessary files on your computer.

5.1.1. Choice of time for updating

The application will inform you when the anti-virus database requires an update. You can also make your own conclusion regarding the updates after reviewing their status in the right frame of the **Protection** tab (see Figure 2).

The status of updates is indicated by the following icons:



– Either no updating of anti-virus database is required or the updating procedure is currently running.



– An update for the anti-virus database is necessary. If updates are unavailable because the license has expired, the program provides relevant information about license extension.



– An update is urgently required; the anti-virus database is either obsolete or missing.

5.1.2. Update procedure



In order to launch the updating process manually,

use the [Update now](#) hyperlink in the left frame of the **Protection** tab

or:

the [update the anti-virus database](#) hyperlink from the notification about the status of the anti-virus database in the right frame of the **Protection** tab;

or:

select the **Update the anti-virus database** item in the pop-up menu, which appears when you right-click the program icon in the system tray.

Clicking a hyperlink opens a window (see Figure 5) containing information on the progress of updating the anti-virus database and application modules.

The procedure for downloading updates can be divided into the following steps:

1. The program obtains a list of updates and information on their size from the Kaspersky Lab update service.
2. Then the program compares the status of the anti-virus database on your computer with the information provided by the update service. If your computer has the latest version of the anti-virus database, you'll see a notification window confirming that the current version of your anti-virus database is up-to-date.
3. The **Updates size** field of the **Update** dialog box (see Figure 5) shows the total size of the updates required for the anti-virus database. If no updates are necessary, the updating procedure is complete. Otherwise, it begins copying files from the Kaspersky Lab update servers of Kaspersky Lab via the Internet. The download progress is reflected by the progress indicator. Besides, the **Total downloaded** field shows the size (in kilobytes) of the updates that have already been downloaded. Upon completion of the download

procedure, the database updates will be installed to your computer automatically.

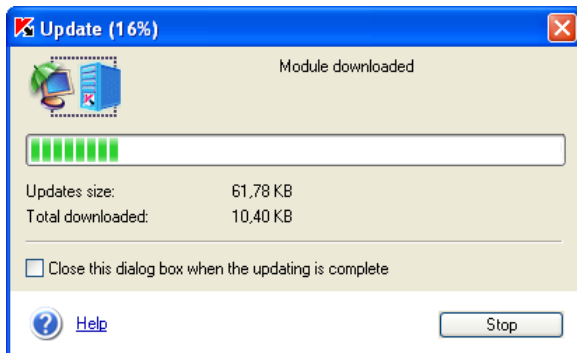


Figure 5. Updating the anti-virus database and application components

5.2. How to prevent a virus infection

Even the most reliable and cautious steps cannot ensure 100% protection against computer viruses and Trojans, but you can minimize the risk of being infected by a virus attack and thus reduce the losses from possible infection.

As in health care, the most efficient way to fight viruses is to prevent a virus infection. Computer virus prevention entails following a few rules in order to reduce the probability of virus infection and data loss.

The key security rules to help prevent viruses from getting onto your computer are listed below.

Rule 1: *Constantly keep your computer protected from viruses using anti-virus programs and Web shields (firewalls). To do this:*

- Install Kaspersky Anti-Virus.
- To keep your virus protection up to date, update your anti-virus database every day. During virus epidemics, you can retrieve updates several times a day because the anti-virus database on Kaspersky Lab servers is updated more than once a day.
- We also recommend that you install Kaspersky Anti-Hacker for comprehensive computer protection while you are surfing the Internet.

Rule 2: *Be careful when introducing any new data onto your computer:*

- Always scan all removable media (floppy disks, CDs, flash cards, etc.) for viruses before using them.

- Be careful with e-mail messages. Never open an e-mail attachment, even one sent to you by someone you know, unless you are certain that it is one you have requested or expected to receive. Especially do not trust e-mails sent by “bogus” anti-virus manufacturers.
- Be cautious when downloading from the Internet. Never download software without a security certificate.
- If you download an executable file from either the Internet or LAN, scan it with Kaspersky Anti-Virus.
- Be selective about the websites you visit. Some websites contain dangerous script viruses or Internet worms.

Rule 3: *Pay attention to information from Kaspersky Lab.*

Kaspersky Lab experts warn users about the beginnings of a new epidemic long before it reaches its peak. If you protect yourself in time with current updates, it will help you avoid infection by any new virus.

Rule 4: *Be wary of virus rumors – e-mail hoax messages that claim to be warnings of real virus threats.*

Rule 5: *Regularly update Windows using the Windows Update utility.*


Rule 6: *Always buy licensed copies of software from official distributors.*

Rule 7: *Limit the number of people who have access to your computer.*

5.2.1. When do I need to scan my computer and particular objects?

Kaspersky Anti-Virus can scan the entire computer for viruses, or particular objects: hard and removable drives, folders, files, or e-mail.

Note that receiving positive results from scanning particular objects on-demand does not guarantee that your computer is free of viruses. Therefore, Kaspersky Anti-Virus always keeps an eye on whether your computer has been completely scanned for viruses.

After a full scan, the program scans more objects stored on your computer than it does in the real-time protection mode. Therefore, for prevention purposes, it is enough to scan your computer at least once a week. The program will remind you when it is better to launch a full scan. If the program main window is closed, a message with a recommendation to start a full scan will pop up above the Kaspersky Anti-Virus icon  in the system tray.

To read more complete information, open the main program window and see the full scan status in the right frame of the program main window on the **Protection** tab (see Figure 2). The following full scan statuses are possible:



– We strongly recommend performing a full scan immediately.



– We recommend performing a full scan using the recommended settings.




– A full scan has been completed recently or is being performed at the moment.

If necessary, you can launch a full scan directly from the full scan status area by clicking [perform full scan](#).

5.2.2. Full scan



To launch an on-demand full scan of your computer for viruses:

click [Scan My Computer](#), in the left frame of the **Protection** tab (see Figure 2). The same action can be executed by clicking [perform full scan](#) in the right part of the **Protection** tab. Also you can use **Scan My Computer for viruses** item in the pop-up menu, which appears when you right-click the  program icon in the system tray.

After clicking this hyperlink, you will see the **Scanning** dialog box (see Figure 4), in which you can view the percent complete of scanned objects, the time elapsed since the start of the scan, the estimated and real time remaining until the end of the scan, and the name of the object scanned.

You can view a report on the program performance (see section 5.4.2 on p. 37, about reporting).

5.2.3. On-demand scans of selected files or folders

There are situations when you need to scan particular objects rather than the entire computer. These objects might be, for example, hard drives with program files and games, e-mail database that you have brought from work, an archive received as an attachment, etc. You can set objects to be scanned using both Kaspersky Anti-Virus options and the standard tools of the Windows operating system (for example, **Explorer**, **My Computer**, etc.).



To define an object to be scanned using standard Windows applications,

select the object and click your right mouse button. The Windows shortcut menu will appear. In this menu, select the **Scan for viruses** command (see Figure 6).

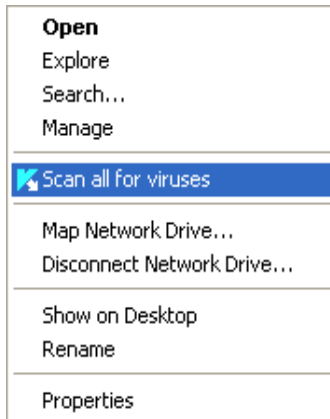


Figure 6. Scanning an object from the Windows shortcut menu



Before selecting an object to be scanned from the Windows shortcut menu, do not forget to install Kaspersky Anti-Virus!



*In order to launch the on-demand anti-virus scan procedure of an object or removable drives, select the following in the left part of the **Protection** tab:*

- [Scan removable drives](#) starts a scan of removable drives;
- [Scan object\(s\)](#) – here you should select an object (file, folder, or disk) and launch the procedure of its scanning. You will see a new window entitled **Select objects to be scanned** (see Figure 7) and containing a list of objects available for scanning and buttons for editing the list and scan control.

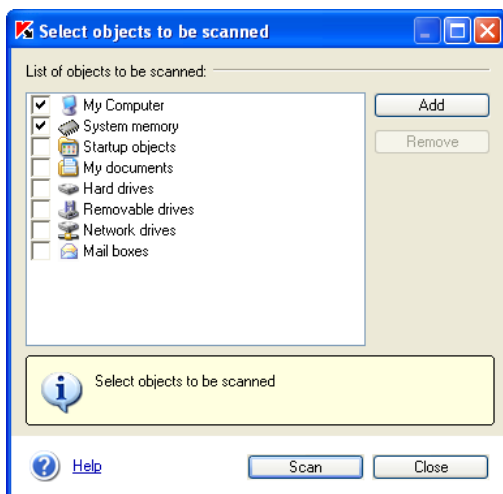



Figure 7. Selection of scanned objects

To add a new file or a folder to the list, click **Add** and browse for the desired file or folder. All added objects will be available in this list for future scans.

To delete an object from the list, check the corresponding box  and click **Remove**. Note that although you can delete added objects from the list, the initial objects cannot be deleted.



To scan objects from the list:

1. Check the corresponding boxes.
2. Click **Scan**.

Regardless of the method of selecting objects to be scanned for viruses (from Kaspersky Anti-Virus or the Windows shortcut menu), the **Scanning** dialog box will appear (see Figure 4). In this box, you can view the percent complete for scanned objects, the time since the scan began, the estimated time until scan completion, and the name of the scanned object being scanned.

You can view a report on program performance (see section 5.4.2 on p. 37).

5.2.4. Scan of archives

Kaspersky Anti-Virus scans archives in the on-demand mode at the **Maximum protection** and **Recommended** protection levels, provided that no exclusions are set (for more information, please contact your security administrator).



Please note that Kaspersky Anti-Virus does not disinfect multivolume archives. When such objects are detected, it will display a window with a **Skip** recommended action command.

If an archive is password protected, the program will ask for the password before scanning objects in the archive (see Figure 8).



Figure 8. Entering a password to scan a protected archive

In the **Enter password** entry field, enter the password for the objects in archive being scanned and click **OK**. The program will continue scanning the archive and objects in it after the password has been entered.

To scan another password-protected archive, Kaspersky Anti-Virus automatically applies the password for the objects in the first archive to the second archive to be scanned. If the password is wrong, you will be asked to enter a new password.

If you do not know the password, the program will be unable to scan the password-protected objects in the archive. We recommend that you click **Skip** and proceed with the scan.

Click the **Skip archive** button to skip all password-protected objects inside an archive being scanned during the current scanning procedure. In doing so, all other objects inside the archive which are not encrypted will be scanned and processed in accordance with the settings defined for anti-virus scanning.




Apply to all password-protected objects within this session means that the selected action will be applied to all password-protected objects in the archive discovered while the current task is running. For example, if you have checked this box and then select **Skip**, **Skip archive**, then the remaining password-protected objects will not be scanned. Or, if you enter the password and click **OK**, then the Anti-Virus will attempt to apply that password to all the remaining encrypted objects and will not display a dialog box.

5.2.5. Treating suspended objects

The necessity of managing infected objects appears if the administrator selected the *Prompt user for action when the scan is completed* variant as the anti-virus action and any infected or suspicious objects are subsequently detected during the scanning procedure.

After completion/termination of the scanning procedure the anti-virus will display the **Managing infected objects** window (see Figure 10), where you can select the actions to be performed over such objects. You can also access the management window for objects to be processed later directly from the scanning progress window (see Figure 4) using the [Detected viruses](#) hyperlink.

When scheduled anti-virus scanning tasks running in the background reveal infected or suspicious objects, a list of the tasks will be shown in the window (see Figure 9) and will be displayed upon clicking the  [Viruses detected...](#) hyperlink in the right frame of the **Protection** tab. In order to review and handle objects set for delayed processing, select the corresponding task from the list and click the **Objects...** button.

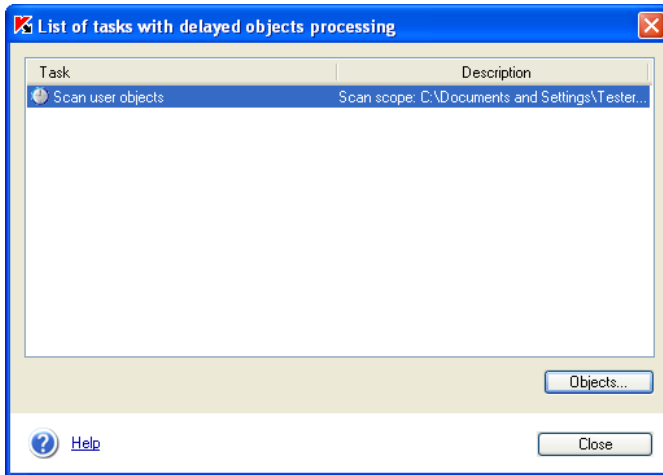


Figure 9. The list of tasks with objects left for later processing

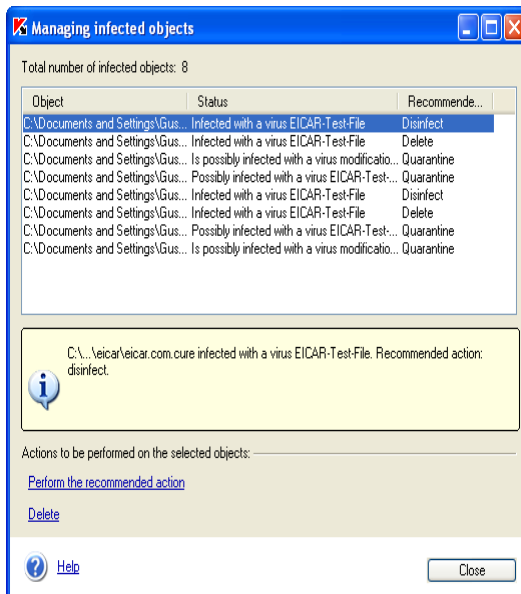


Figure 10. Management window for infected and suspicious objects



Note that scanning and disinfection of password-protected objects in archives are **NOT PERFORMED** in the delayed treatment mode.

In this dialog box, you can see a list of infected and suspicious objects found during the scan (see Figure 10). The **Object** column contains the path and the name of each object, the **Status** column its status, and the **Recommended action** column shows the action recommended by Kaspersky Lab experts for the object.

In order to select an object and perform a certain action on it, you should check its box. You can select several listed objects at once. All the objects in the list can be selected by checking the box in the list header.

You can apply one of the following actions to the listed files:

- [Perform the recommended action](#) – Apply the action recommended by Kaspersky Lab experts. The recommended action for infected objects is **disinfect** or **delete** and the action for suspicious objects is **quarantine**.
- [Delete](#) – Delete a file.

After an action is applied, the program will open a dialog box displaying the action in progress. You can always stop the action by clicking **Stop**.

Processed objects will be deleted from the list. After all listed objects have been processed, click **Close**.

5.2.6. How to scan a CD or a floppy disk

Your computer can easily be infected by viruses on floppy disks, CDs, and other removable media. If you have used a floppy disk (or a bootable CD) infected with a boot virus, or have left it in your floppy drive and rebooted, this may cause serious problems with your system.

We recommend that you scan all removable media before using them.

You can scan removable media either from the Kaspersky Anti-Virus main window or by using the Windows shortcut menu, accessed from **Explorer**, **Desktop**, etc.



To scan removable media for viruses from the Windows shortcut menu,

select the medium (you can select a CD and a floppy disk at the same time) and click your right mouse button. The Windows shortcut menu will appear. In this menu, select **Scan for viruses** (see Figure 6).



To scan a CD or a floppy disk for viruses from the Kaspersky Anti-Virus main window:

1. Insert a CD into the CD-ROM drive or a floppy disk into the floppy drive.
2. Click [Scan removable drives](#) in the left frame of the **Protection** tab (see Figure 2).

After the scan of selected objects is launched, you can view the scanning percentage in the **Scanning** dialog box (see Figure 4).



Note the following specific features of program performance:

- If you forget to put a CD or a floppy disk into the drive, or your CD-ROM drive or floppy drive is disconnected, the scan will fail without any additional notification.
- If you put a floppy disk into the floppy drive after you launch the scan, the program will not scan this floppy disk. The same is true for CDs and other removable media.
- If you have taken a floppy disk out of the floppy drive or disconnected the floppy drive during scanning, the program will report an error but will not provide any additional notification. After this, the program will scan the next removable drive if such exists on your computer.

5.3. Real-time protection

Real-time protection means a mode of the Anti-Virus operation wherein it constantly resides in computer RAM, monitoring all calls to file system objects and actions of potentially dangerous VBScript and JavaScript scripts as well as macro commands used in office applications and detects potentially dangerous software.

Before access to an object is granted, the program scans it for viruses, and, if a virus is detected, it disinfects or removes the object or blocks access to it (depending on the settings you have defined). Thus, the application allows detection and removal of malicious code prior to actual system infection.

By default, real-time protection remains active from the moment that the operating system is loaded until you finish working with the computer.

Information about the current status of real-time protection is displayed in the right frame of the **Protection** tab (see Figure 2) in the Kaspersky Anti-Virus main window.

The status of real-time protection is denoted by the following icons:





– Real-time protection is enabled. The protection level of your computer is set to Recommended.



– Real-time protection is disabled. The settings of real-time protections differ from Recommended.



– Real-time protection is disabled or is not being performed.

Switching of the active  icon (red) to inactivated  (gray) condition confirms that real-time protection is disabled.

5.4. Additional features

Kaspersky Anti-Virus offers several additional options for product use, including:

- Relocation of suspicious objects to quarantine storage.
- Operations with copies of objects deleted or modified by the Anti-Virus and located in the backup storage.
- Viewing the application operation report.

5.4.1. Quarantine and Backup storage

Kaspersky Anti-Virus gives users the option of isolating suspicious objects in quarantine or preserving copies of infected objects located in the backup storage prior to their disinfection or removal.

When a suspicious object is detected, the application isolates it in a quarantine directory, where the object can be rescanned, deleted, restored, or sent to Kaspersky Lab for analysis.

The application creates a backup copy upon object detection before the first attempt of its disinfection or removal; the copy is saved to backup directory, from which the object may be restored later if it contains valuable data.

5.4.1.1. Work with Quarantine storage

By default, Kaspersky Anti-Virus moves all suspicious objects detected during full computer scan or in the real-time protection mode to quarantine, where you may continue working with them (scanning, restoring, deleting, etc.).

Kaspersky Anti-Virus rescans quarantined objects after each update of its anti-virus database. If you need to scan quarantined objects manually, we recommend updating the anti-virus database prior to the scan. Updated database may already contain information about viruses suspected in your files, and in that case, they might be disinfected.

Thus, work with suspicious files is performed in the **Quarantine** window (see Figure 11), which is opened by clicking the [Quarantine](#) hyperlink on the **Protection** tab (see Figure 2) of the main program window or the [View Quarantine](#) hyperlink in the complete scan window (see Figure 4).

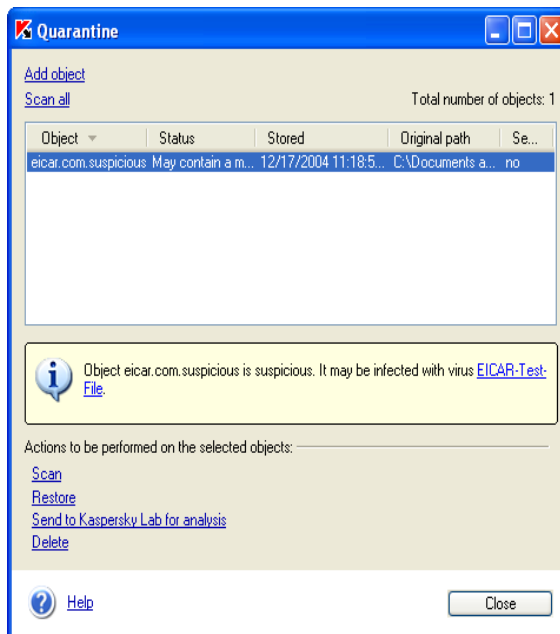


Figure 11. Quarantine storage window

In this dialog box you can perform the following operations in the quarantine storage:

- Quarantine a file which you suspect of containing a virus, even though it has not been detected by the Anti-Virus. In order to do so, use the [Add object](#) hyperlink and select the suspicious file in the standard browsing window. It will be transferred to the list from its original location.
- Scan and disinfect all suspicious files or files selected from a list using the current anti-virus database. In order to do so use the [Scan all](#) hyperlink or [Scan](#) hyperlink (having first selected the files to scan). Scanning and disinfecting any quarantined object may change its status to *infected* or *dis-*

infected.

The *infected* status means that the object has been identified as infected, but disinfection failed. We recommend deleting objects with this status.

All objects with *false alarm* status can be restored without hesitation, because their previous *possibly infected* status was erroneously assigned by Kaspersky Anti-Virus.



By default, files in the quarantine directory are scanned automatically after each update of the anti-virus database.

- Restore the files to the same directories from which they were moved to quarantine or to a specified destination folder (depending upon administrator's settings). In order to restore an object, select it in the list and use the [Restore](#) hyperlink.



We recommend only restoring objects with *false alarm* status, because restoring of other objects may cause infection of your computer.

- Send suspicious objects to experts at Kaspersky Lab for examination. We recommend sending an object for expert appraisal only in cases when its status does not change after several attempts of its scanning and disinfection. Use the [Send to Kaspersky Lab for analysis](#) hyperlink to do so.
- Delete any quarantined file or a selected group of files. Only remove files which cannot be disinfected. In order to remove a file, select it in the list and use the [Delete](#) hyperlink.

5.4.1.2. Work with Backup storage

Kaspersky Anti-Virus always creates copies of infected or suspicious objects before their disinfection or removal; the copies are saved to the Backup storage directory.

When necessary, you can restore any object if, for instance, its disinfection resulted in data loss, if the object has been erroneously deleted, or if you plan to reattempt disinfection using the updated anti-virus database.

Work on backup copies is performed in the **Backup** window (see Figure 12), which opens after clicking the [Backup](#) hyperlink in the **Protection** tab (see Figure 2) of the main application window.

You can perform the following actions in the Backup storage window:

- Restore objects to the original directories from which they have been added to Backup storage or to a specified destination folder (depending upon administrator's settings). In order to restore an object, select it in the list and use the [Restore](#) hyperlink.

- Remove files from the Backup storage. In order to delete a file, select it in the list and use the [Delete](#) hyperlink.

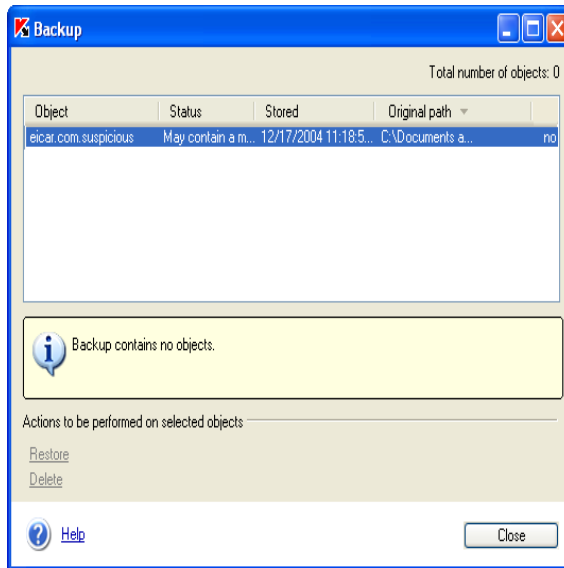


Figure 12. Backup storage window

5.4.2. Work with reports

The application creates reports while performing a full computer scan, updating the anti-virus database and in real-time protection mode appending information to it about scanned objects and the results of their processing, as well as general statistics.

Kaspersky Anti-Virus maintains Task log that contains a comprehensive report of the tasks performed (see Figure 13), which can be reviewed by clicking the [Reports](#) hyperlink in the left frame of the **Protection** tab (see Figure 2). Here it logs the status of each task, together with the date and time of its completion.

The status information about object processing may belong to one of the following variants:

- *Notification of success* (e.g., the object is clear, object was disinfected or deleted).
- *An informational message* (e.g., the task has been launched, completed, in progress or paused).

- *Warning* (e.g., a suspicious object or a password-protected archive was discovered).
- *Critical event* (e.g., a virus was detected) or *Failure* (e.g. because the license period is expired).
- *Functional failure* (e.g., because the period of license validity has expired).

As a rule, notifications of success and informational messages are for reference only and thus they do not have critical importance. You can disable display of task reports which contain only those message types. In order to do so, uncheck the ☒ **Show informational reports** box.

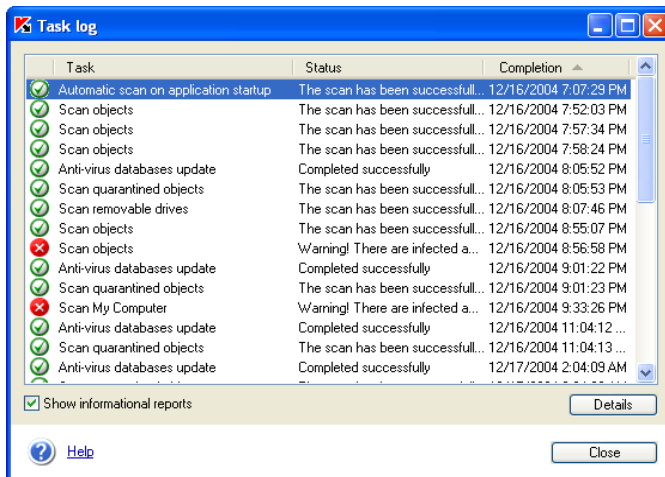


Figure 13. Task log

You can review the settings, statistics and a report on detected objects for any task using the respective tabs if you select it in the log. Click the **Details** button to accomplish that.

Clicking the button will open a window containing a detailed report about task performance represented by the **Statistics**, **Report**, and **Settings** tabs.

Thus the **Statistics** tab (see Figure 14) lets the user review general information about the work performed by the Anti-Virus to accomplish the task: the date and time of task start, the total number of scanned files, and the number of infected, disinfected, and quarantined objects.

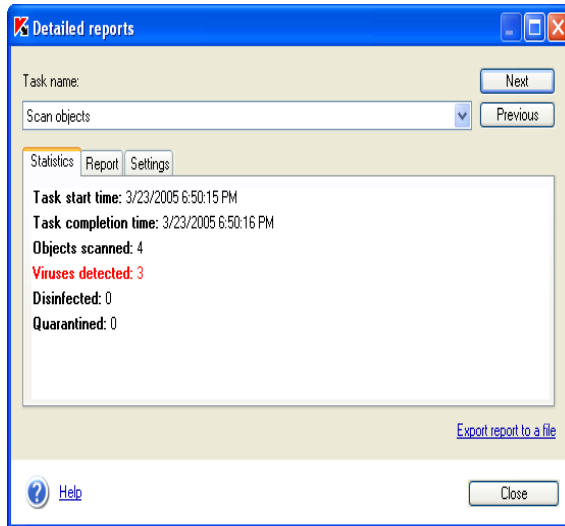


Figure 14. **Statistics** tab

The **Report** tab (see Figure 15) contains detailed information about each scanned object.

The **Settings** tab (see Figure 16) displays task parameters used in scanning. It shows both the scope of the scan and the level of protection defined for the task as well as program actions to be performed with infected or suspicious files. The tab also displays objects excluded from scanning if they have been defined.

You can select the tasks for review either in the **Task log** or directly in the detailed report window using the **Next** and **Previous** buttons or by clicking the task name in the respective drop-down list.

You can also receive the report in the text document format by clicking the [Export report to file](#) hyperlink. Clicking the link will open a standard window. Use it to enter the file name, select the directory on the disk where the file should be stored, and click the **Save** button.

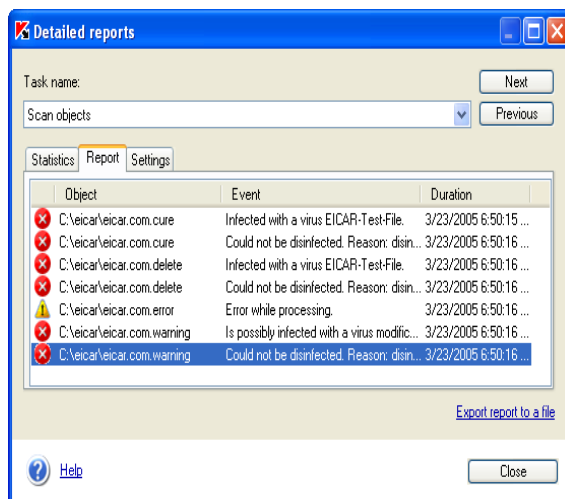


Figure 15. Report tab

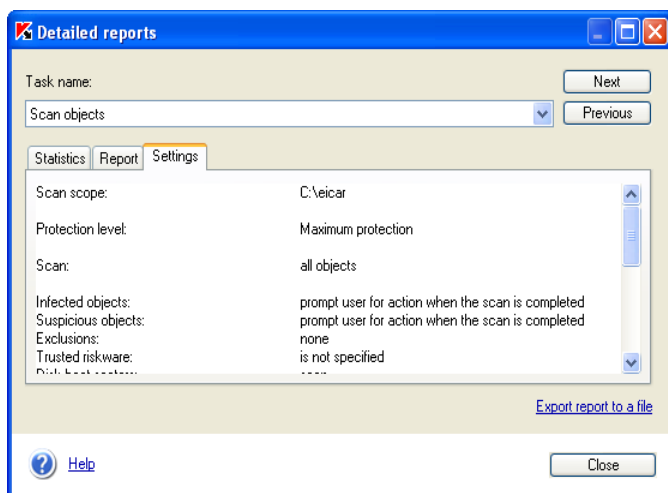


Figure 16. Settings tab

APPENDIX A. FREQUENTLY ASKED QUESTIONS

This chapter is devoted to the most frequently asked questions from users pertaining to installation, setup, and operation of Kaspersky Anti-Virus. We shall try to answer them here in detail.



Question: Is this possible to use Kaspersky Anti-Virus with anti-virus software supplied by other manufacturers?

In order to avoid conflicts we recommend that you uninstall ant-virus software of other manufacturers prior to installation of Kaspersky Anti-Virus.



Question: Kaspersky Anti-Virus does not rescan files that have been scanned earlier. Why?

This is true. Kaspersky Anti-Virus does not rescan files that have not changed since the last scan.

This is possible due to the use of new technologies: iChecker and iStreams. These technologies involve verification of the checksums of the files in the additional NTFS streams.



Why does Kaspersky Anti-Virus cause a certain decrease in server performance, noticeably loading the CPU?

Virus detection is a computationally intensive mathematical problem, requiring structural analysis, checksum calculation and mathematical data conversions. Processor time is therefore the main resource consumed by the anti-virus software, and each new virus added to the anti-virus database increases the overall scanning time. This is a necessary sacrifice for the security and safety of your data.

Other anti-virus products speed up scanning by excluding both viruses which are less easily detectable or less frequent in the geographic location of the anti-virus vendor and file formats that require complicated analysis (e.g. PDF) from their database.

In contrast, Kaspersky Lab believes that the purpose of its anti-virus applications is to establish real and complete anti-virus security for its users. We believe that "partial protection" is even worse than no protection at all, because it forces users to take personal precautions.

Kaspersky Anti-Virus gives its users maximum protection. Experienced users can, of course, accelerate anti-virus scanning to the detriment of

overall security by disabling scanning of various file types, but we do not recommend doing so for users who want the best protection.

For maximum user protection, Kaspersky Anti-Virus recognizes more than 700 formats of archived and compressed files. This is essential for anti-virus security, because harmful executable code may be hidden inside files of any recognized format. However, despite the daily growth in the number of viruses detected by Kaspersky Anti-Virus (approximately 30 new viruses appear daily) as well as the ever increasing number of recognized file formats, each subsequent version of our product functions faster than the previous one. That is achieved through the use of new, exclusive technologies, such as iChecker™ and iStreams™, developed at Kaspersky Lab.



Question: *Why do I need the key file? Will my copy of the anti-virus application work without it?*

No, Kaspersky Anti-Virus does not work without a license key.

If you are still deciding whether or not to purchase Kaspersky Anti-Virus, we can provide you with a temporary key file (trial key), which will only work either for two weeks or for a month. When this period expires, the key will be blocked.



Question: *What happens when the license expires?*

After expiration of the license, Kaspersky Anti-Virus will continue operating, but anti-virus database updating will be disabled. The anti-virus application will continue cleaning infected objects but only using the old anti-virus database.

If such a situation arises, notify your system administrator and contact the company from which you purchased Kaspersky Anti-Virus or Kaspersky Lab directly for license extension.



Question: *My anti-virus application does not work.*

What should I do?

First, check if a solution for your problem is provided in this documentation, especially in this section or on our website.

In addition, we recommend that you apply for support to the distributor from whom you purchased Kaspersky Anti-Virus or write to our Technical support service (support@kaspersky.com) or to the address contained in the license key information.

To make sure your request is answered as soon as possible, follow these suggestions:

1. In the message header, specify your server's operating system, the name of the component you are experiencing problems with, and briefly describe the problem. For example:
MS Windows 2000, Kaspersky Anti-Virus 5.0 for Windows Workstations, anti-virus database updates do not work.
2. Compose your messages in plain text format. Avoid sending HTML messages.
3. At the beginning of the message, specify the exact versions of the operating system and Kaspersky Anti-Virus distribution package and provide the name of your license key file.
4. Clearly describe the problem in brief. Keep in mind that, when reading your mail, the support service officers do not yet know about your problem. They can only help after fully understanding and reproducing it.
5. Send the following data to the Technical support service (pack them in one archive before sending):
 - Anti-virus log file (see section 5.4.2 on p. 37);
 - License key.
6. Make sure to specify in your mail if you have any of the following on your system:
 - SCSI controller;
 - A very old or very new brand of processor, or more than one processor;
 - Less than 64 MB or more than 2 GB of RAM.



Question: *Why are daily updates required?*

Just several years ago computer viruses were distributed via floppy disks and at that time it was sufficient to install an anti-virus program and update your anti-virus database from time to time in order to ensure reliable anti-virus protection of your computer. However, the latest virus outbreaks spread over the world within several hours and if your anti-virus program uses outdated database, it may be helpless against new threats. In order not to fall a victim of viruses, you should update your anti-virus on a daily basis.

Kaspersky Lab updates its anti-virus database more frequently every year. Now it is updated every hour.

Additionally, Anti-virus application modules are updated which eliminates detected vulnerabilities and expands the program's functionality.



Question: *What's new in version 5.0?*

The 5.0 Kaspersky Lab's range of products includes new updating service which was developed in accordance with the requests of our users and the market demands. Additionally, it was done in order to increase flexibility of the entire updating procedure, starting with the updates preparation at Kaspersky Lab through updating the files at the user's computer.

The advantages of the new updating service are as follows:

- *Existing downloads are saved when the connection fails.* Now you will not have to download updates that have been already downloaded, when you lose and restore your internet connection;
- *A 50% reduction in the size of the cumulative update.* The cumulative update contains the entire anti-virus database and is considerably larger than a regular update. The new service utilizes a special technology that allows to use the existing anti-virus database in the cumulative update process.
- *Faster internet downloads.* Kaspersky Anti-Virus now selects a Kaspersky Lab update server located in your region. Besides, the load to the server is now distributed based on the server speed, which means that you will not be directed to an overloaded server while other servers will be idle.
- *The use of black list of license keys.* This allows to prohibit updates to users who do not have Kaspersky Anti-Virus license. Licensed users will not then suffer delays due to overloaded update servers.
- *For corporate products a possibility to arrange a local update server has been implemented.* This function is required for organizations that have several computers connected to one local network and protected with Kaspersky Anti-Virus software. In this case, any computer in the LAN may turned into the update server that will receive updates from the internet, place them into a local folder and allow access to this folder for other computers connected to this local network.



Question: *Is it possible for an intruder to replace the anti-virus database?*

Every anti-virus database has a unique signature checked by Kaspersky Anti-Virus when accessing the database. If the signature is

invalid or the date of the database is later than that of the license expiration, Kaspersky Anti-Virus will not use it.

APPENDIX B. CONTACTING TECHNICAL SUPPORT SERVICE

Kaspersky Anti-Virus provides support through Technical Support Service at Kaspersky Lab in the following cases:

- You believe that the application behaves abnormally and malfunctions.
- Kaspersky Anti-Virus has detected a suspicious file containing information valuable to you and has blocked it. You would like to continue working with the file.



In order to send a message about application malfunctions to the Technical Support Service,

use the [Send question to technical support](#) hyperlink in the left frame of the **Support** tab (see Figure 3) in the main program window.

Clicking the hyperlink will automatically open a window of the mail client installed on your computer, e.g. MS Outlook, and create an e-mail message including a text file with description of your system and all necessary data pertaining to Kaspersky Anti-Virus. Please describe in detail the problem which you encountered while working with Kaspersky Anti-Virus and send the message. The support team will contact you as soon as possible.

If Kaspersky Anti-Virus has quarantined a suspicious file, you may update the anti-virus database and attempt disinfecting it (see section 5.4.1.1 on p. 34). However, if the object cannot be disinfecting, but you wish to recover it as soon as possible, you may send the object for examination to Kaspersky Lab. The file may really be infected with an unknown virus type, or a false alarm might have occurred.



In order to send a message to the Technical Support Service using the automated system of user feedback processing,

Click the [Help us to make this product better!](#) hyperlink in the left frame of the Support tab in the main program window (see Figure 3).

Clicking the link will launch MS Internet Explorer and open a feedback collection form on the web site of Kaspersky Lab. Please fill all obligatory fields and add your inquiry. The specialists at the Technical Support Service will process it and reply as soon as possible.



In order to send an individual suspicious file for examination to Kaspersky Lab,

select the suspicious file in the **Quarantine** window (see section 5.4.1.1 on p. 34) and use the [Send to Kaspersky Lab for analysis](#) hyperlink.

Clicking the hyperlink will automatically open a window of the mail client installed on your computer, e.g. MS Outlook Express, and create an e-mail message with the suspicious file attached. Send the message. Experts at Kaspersky Lab will closely examine the file you have sent and attempt to recover all the data in it. You will receive a full report regarding the results of file examination.



Please note that you may send no more than three files to Kaspersky Lab for examination within one day. Each file must have been scanned by Kaspersky Anti-Virus with a database updated no more than three days before it is sent.

It may happen that Kaspersky Anti-Virus does not detect files that you are absolutely confident are infected with a new virus type during scanning. Such files can also be sent to Kaspersky Lab for examination.



In order to send the files which you suspect of virus infection for further examination at Kaspersky Lab,

use the [Send file for analysis](#) hyperlink in the left frame of the **Support** tab (see Figure 3). Indicate the suspicious files in the standard browsing window.

The procedure of sending an e-mail message to Kaspersky Lab is absolutely identical to the one described for sending suspicious quarantined objects.

APPENDIX C. GLOSSARY

These documents use terms and concepts specific to the field of anti-virus protection. This glossary serves as a dictionary containing definitions for those concepts. For convenience, the glossary is arranged in alphabetic order.

A

Anti-virus database – a database created by Kaspersky Lab specialists that contains detailed descriptions of all currently existing viruses and methods for their detection and disinfection. Our anti-virus database is regularly updated with information about new viruses; therefore, to keep your computer constantly protected from viruses, you need to keep your anti-virus database updated.

Anti-virus protection status – current status of anti-virus protection that characterizes the security level for your computer.

B

Backing up – creating a backup of a file in the backup storage folder before treating it (disinfection or deleting). This file can later be restored from its backup, for example, for subsequent scanning with the current version of the anti-virus database.

Backup storage – a special storage area designed to preserve backup copies of objects made prior to their disinfection or removal.

"Black list" – the database containing the information about license keys belonging to owners who have committed violations of the License Agreement, and about keys that have been generated but remained unsold for some reason. The content of the black list is updated along with the anti-virus database; Kaspersky Anti-Virus will not work without it.

C

Current license key - the license key installed and currently used by Kaspersky Anti-Virus to unlock its functionality. It determines the period of license validity and licensing policy regarding the product. An application cannot have more than one key with "current" status.

D

Deleting an object – a method of treating an object. To delete an object is to remove it physically from a computer. This method is recommended for treating infected objects. If deleting is the first action applied to an object, it is necessary to create a backup copy of this object before deleting it. You can use the backup to restore the original object.

Disinfection – a method of treating *infected objects*. Disinfection implies partial or full recovery of data or results in a decision that these files cannot be disinfected. Objects are disinfected using the anti-virus database. If disinfection is the first action to be applied to an object, i. e. the

first action after detection of a suspicious object, the application creates a backup copy of this file. If some data are lost during disinfection, you can use the backup to recover this object.

Disinfection of objects at restart – a method of processing infected objects which are being accessed by other applications while the application attempts their disinfection. The application creates a copy of the infected object, disinfects the copy, and substitutes it for the original infected object during the next restart. In MS Windows 9x operating systems, disinfection of objects with long filenames during restart forces their replacement with disinfected objects having short filenames. That may cause incorrect functioning of applications, which use objects disinfected in this manner.

E

E-mail database – database that contains e-mail messages stored on your computer. Every incoming/outgoing message is saved in the database after you receive/send it. Such database is scanned in the on-demand scanning mode.

Exclusions – user-defined settings that exclude certain objects from the scan. You can customize the exclusion rules for real-time protection and on-demand scans. Thus, you can disable scanning of archives during a full scan or exclude files from scans by using masks.

F

Full scan – a mode of application functioning designed for full computer scanning for the presence of malicious code upon a request made by the user with subsequent disinfection and removal of suspicious or infected objects, if any.

H

High speed – a level of computer security which provides top system performance at the expense of lower anti-virus protection.

I

Infected object – an object containing harmful code. We recommend that you abandon working on these objects because they can infect your computer.

L

License key – a file with the .key extension that serves as your personal "key". This file is required for correct operation of Kaspersky Anti-Virus. The license key is included in the distribution kit if you purchased your copy of Kaspersky Anti-Virus from Kaspersky Lab distributors. If you purchased the product online, the license key is sent to you via e-mail. Without the license key, Kaspersky Anti-Virus DOES NOT WORK.

License period – the period during which you have the right to use the full functionality of Kaspersky Anti-Virus. As a rule, the license period defined by the license key is one calendar year from the date of license

key activation. After your license expires, the product will operate, but you will not be able to update the *anti-virus database* and *application modules*.

M

Maximum protection – the level of computer security which corresponds to maximum possible protection, leading to a certain performance decrease.

O

OLE object – objects or documents embedded in other files using the OLE technology.

Q

Quarantine – a special data storage designed for isolation of suspicious objects.

Quarantining (moving to a quarantine folder) – a method for treating a *suspicious object* which involves blocking access to the object and moving it to a quarantine folder for subsequent treatment.

R

Real-time protection – a mode of application functioning in which the application resides permanently in computer memory and monitors calls to file system objects. Prior to granting access to an object, the application scans it for virus presence and, if a virus is detected, the application dis-infects the object or removes it or blocks access to it (depending upon the settings you have defined).

Recommended level – the default level of anti-virus protection with settings recommended by Kaspersky Lab experts which ensures the optimal balance between performance and protection.

Recovering, restoring – moving an original file from the *quarantine* or *backup* folders to a specified destination folder or to its original location, where it was stored before quarantining, disinfection, or deleting.

Reserved license key – a license key which has been installed to enable proper functionality of Kaspersky Anti-Virus but has not yet been activated. This reserved key will be activated as soon as the license provided by the current key expires.

S

Startup objects – a set of programs that are necessary for launching and correct operation of the operating system and other programs installed on your computer. Your operating system launches these objects during each startup. Some viruses attempt to infect the startup objects and can cause a startup failure.

Suspicious object – an object that contains either a modified code of a well-known virus or a code reminiscent of a virus, but not yet known to Kaspersky Lab.

U

Unknown virus – a new virus that is not recorded in the *anti-virus database*.

As a rule, Kaspersky Anti-Virus detects unknown viruses using a *heuristic code analyzer* and objects containing these viruses are identified as *suspicious*.

Update – the procedure of replacement/addition of new files (the anti-virus database or application modules) downloaded from Kaspersky Lab update servers.

V

Virtual drives (RAM drives) – RAM area in a personal computer which emulates a regular physical computer disk.

APPENDIX D. KASPERSKY LAB

Founded in 1997, Kaspersky Lab has become a recognized leader in information security technologies. It produces a wide range of data security software and delivers high-performance, comprehensive solutions to protect computers and networks against all types of malicious programs, unsolicited and unwanted e-mail messages, and hacker attacks.

Kaspersky Lab is an international company. Headquartered in the Russian Federation, the company has representative offices in the United Kingdom, France, Germany, Japan, USA (CA), the Benelux countries, China and Poland. A new company department, the European Anti-Virus Research Centre, has recently been established in France. Kaspersky Lab's partner network incorporates more than 500 companies worldwide.

Today, Kaspersky Lab employs more than 250 specialists, each of whom is proficient in anti-virus technologies, with 9 of them holding M.B.A. degrees, 15 holding Ph.Ds, and two experts holding membership in the Computer Anti-Virus Researchers Organization (CARO).

Kaspersky Lab offers best-of-breed security solutions, based on its unique experience and knowledge, gained over more than 14 years of fighting computer viruses. A thorough analysis of computer virus activities enables the company to deliver comprehensive protection from current and even future threats. Resistance to future attacks is the basic policy implemented in all Kaspersky Lab's products. At all times, the company's products remain at least one step ahead of many other vendors in delivering extensive anti-virus coverage for home users and corporate customers alike.

Years of hard work have made the company one of the top security software manufacturers. Kaspersky Lab was one of the first businesses of its kind to develop the highest standards for anti-virus defense. The company's flagship product, Kaspersky Anti-Virus®, provides full-scale protection for all tiers of a network, including workstations, file servers, mail systems, firewalls and Internet-gateways, hand-held computers. Its convenient and easy-to-use management tools ensure advanced automation for rapid virus protection across an enterprise. Many well-known manufacturers use the Kaspersky Anti-Virus® kernel, including Nokia ICG (USA), F-Secure (Finland), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India), BorderWare (Canada), etc.

Kaspersky Lab's customers benefit from a wide range of additional services that ensure not only stable operation of the company's products but also compliance with any specific business requirements. Kaspersky Lab's anti-virus database is updated in real-time every 3 hours. The company provides its customers with a 24-hour technical support service, which is available in several languages to accommodate its international clientele.

D.1. Other Kaspersky Lab Products

Kaspersky Anti-Virus® Personal

Kaspersky Anti-Virus® Personal protects home computers running Windows 98/ME/2000/NT/XP from all types of known viruses, including Riskware. The application constantly monitors all possible sources of virus penetration, such as e-mail, Internet, floppy disks, CDs, etc. Unknown viruses are efficiently detected and processed by a unique heuristic data analysis system. The two distinct modes of the application's operation (that can be used either separately or jointly) are:

- **Real-Time Protection** – anti-virus scan of all files being run, opened or saved on the protected computer.
- **On-Demand Scan** – scanning and disinfection of the entire computer or individual disks, files or folders. You can launch a scan manually using the graphical interface or set up a regular scheduled scan.

Kaspersky Anti-Virus Personal does not scan objects already analyzed during previous scans that have not been modified since then. This rule now applies not only to the real-time protection but also to the on-demand scan. This feature **greatly improves the speed and performance of the application**.

Kaspersky Anti-Virus Personal provides reliable protection against viruses that attempt to penetrate computers via e-mail messages. The application provides automatic scanning and disinfection of all incoming (POP3) and outgoing (SMTP) e-mail messages and efficiently detects viruses in e-mail database.

Kaspersky Anti-Virus Personal supports over 700 formats of archived and compressed files and ensures automatic anti-virus scanning of their content and removal of malicious code from files within **ZIP**, **CAB**, **RAR** and **ARJ** archives.

The application's settings can easily be adjusted to one of the three pre-defined levels: **Maximum Protection**, **Recommended Protection** and **Maximum Speed**.

The anti-virus database is updated every three hours. Database delivery is guaranteed even if the internet connection is interrupted or switched during the download process.

Kaspersky Anti-Virus® Personal Pro

This package has been designed to deliver comprehensive anti-virus protection to home computers running Windows 98/ME, Windows /2000/NT, Windows XP as well as MS Office applications. Kaspersky Anti-Virus® Personal Pro includes an application for automatic retrieval of daily updates to the anti-virus database and the application modules. A second-generation heuristic analyzer efficiently detects unknown viruses. Simple and user friendly interface of the program

allows easy settings modifications providing maximum comfort for the program's user.

Kaspersky Anti-Virus® Personal Pro features:

- **on-demand scans** of local disks initiated by the user;
- **automatic real-time protection** that involves the scan of all running files;
- **mail filter** that automatically scans and disinfects all incoming (POP3) and outgoing (SMTP) messages and provides reliable and efficient virus detection in e-mail databases;
- **behavior blocker** that guarantees 100% protection against MS Office applications macro viruses.
- **anti-virus scan** of over 900 versions of archived and compressed files formats, anti-virus scan of files contained in such objects and removal of malicious code from **ZIP, CAB, RAR and ARJ** files.

Kaspersky® Anti-Hacker

Kaspersky® Anti-Hacker is a personal firewall that is designed to safeguard a computer running any Windows operating system. It protects your computer against unauthorized access and external hacker attacks from either the Internet or the local network.

Kaspersky® Anti-Hacker monitors the TCP/IP network activity of all applications running on your machine. When it detects a suspicious action, the application blocks the suspicious application from accessing the network. This helps deliver enhanced privacy and 100% security of confidential data stored on your computer.

The product's SmartStealth™ technology prevents hackers from detecting your computer from the outside. In this stealthy mode, the application works seamlessly to keep your computer protected while you are on the Web. The application provides conventional transparency and accessibility of information.

- Kaspersky® Anti-Hacker also blocks most common network hacker attacks and monitors for attempts to scan computer ports.
- Configuration of the application is simply a matter of choosing one of five security levels. By default, the application starts in self-learning mode, which will automatically configure your security system depending on your responses to various events. This makes your personal guard adjustable to your specific preferences and your particular needs.

Kaspersky® Security for PDA

Kaspersky® Security for PDA provides reliable anti-virus protection of data stored on PDAs running Palm OS or Windows CE. It also offers anti-virus protection from any corrupted files transferred from a PC or an extension card, from ROM

files, and from database. This software package includes an optimal combination of the following anti-virus tools:

- **anti-virus scanner** to scan the data stored on both the PDA and extension card on demand;
- **anti-virus monitor** to intercept viruses in files that are either copied from other handhelds or are transferred using HotSync™ technology.

Kaspersky® Security for PDA protects your handheld (PDA) from unauthorized intrusion by encrypting both access to the device and data stored on memory cards.

Kaspersky Anti-Virus® Business Optimal

This package provides a configurable security solution for small- and medium-sized corporate networks.

Kaspersky Anti-Virus® Business Optimal includes full-scale anti-virus protection¹ for:

- *Workstations* running Windows 98/ME, Windows NT/2000/XP Workstation, and Linux;
- *File and application servers* running Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Windows 2003 Server, Novell Netware, FreeBSD and OpenBSD, and Linux;
- *E-mail clients*, namely Microsoft Exchange 5.5/2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail, and Qmail;
- *Internet-gateways*: CheckPoint Firewall –1; MS ISA Server.

The Kaspersky Anti-Virus® Business Optimal distribution kit includes Kaspersky® Administration Kit, a *unique tool for automated deployment and administration*.

You are free to choose from any of these anti-virus applications, according to the operating systems and applications you use.

Kaspersky® Corporate Suite

This package provides corporate networks of any size and complexity with comprehensive, scalable anti-virus protection. The package components have been developed to protect every tier of a corporate network, even in mixed computer environments. Kaspersky® Corporate Suite supports the majority of operating systems and applications installed across an enterprise. All package components are managed from one console and have a unified user interface. Kaspersky® Corporate Suite delivers a reliable, high-performance protection system that is fully compatible with the specific needs of your network configuration.

¹ Depending on the type of distribution kit.

Kaspersky® Corporate Suite provides comprehensive anti-virus protection for:

- *Workstations* running Windows 98/ME, Windows NT/2000/XP, and Linux;
- *File and application servers* running Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD and Linux;
- *E-mail clients*, including Microsoft Exchange Server 5.5/2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim and Qmail;
- *Internet-gateways*: CheckPoint Firewall –1; MS ISA Server;
- *Hand-held computers* (PDAs), running Windows CE and Palm OS.

The Kaspersky® Corporate Suite distribution kit includes Kaspersky® Administration Kit, a *unique tool for automated deployment and administration*.

You are free to choose from any of these anti-virus applications, according to the operating systems and applications you use.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam is a cutting-edge software suite that is designed to help organizations with small- and medium-sized networks wage war against the onslaught of undesired e-mail (spam). The product combines the revolutionary technology of linguistic analysis with modern methods of e-mail filtration, including RBL lists and formal letter features. Its unique combination of services allows users to identify and wipe out up to 95% of unwanted traffic.

Installed at the entrance to a network, where it monitors incoming e-mail traffic streams for spam, Kaspersky® Anti-Spam acts as a barrier to unsolicited e-mail. The product is compatible with any mail system and can be installed on either an existing mail server or a dedicated one.

Kaspersky® Anti-Spam's high performance is ensured by daily updates to the content filtration database by samples provided by the Company's linguistic laboratory specialists.

Kaspersky® Anti-Spam Personal

Kaspersky® Anti-Spam Personal is designed to protect users of mail client programs Microsoft Outlook and Microsoft Outlook Express against unwanted e-mail messages (spam).

Kaspersky® Anti-Spam Personal software package is a powerful tool that ensures detection of spam in the flow of e-mail messages incoming via POP3 and IMAP4 protocol (only for Microsoft Outlook).

The filtering process involves the analysis of all attributes of the message (sender's and recipient's addresses and headers), content filtration (analysis of

the content of the letter, including the Subject and attached files), as well as unique linguistic and heuristic algorithms.

The application's high performance is enhanced by daily updates to the content filtration database by samples provided by the Company's linguistic laboratory specialists.

D.2. Contact Us

If you have any questions, comments, or suggestions, please refer them to one of our distributors or directly to Kaspersky Lab. We will be glad to assist you in any matters related to our product by phone or via e-mail. Rest assured that all of your recommendations and suggestions will be thoroughly reviewed and considered.

Technical support	Please find the technical support information at http://www.kaspersky.com/supportinter.html
General information	WWW: http://www.kaspersky.com http://www.viruslist.com E-mail: sales@kaspersky.com

APPENDIX E. INDEX

Anti-virus database updating, 42

Backup

work with files, 36

Box package

buy offline, 12

License agreement, 12

License key, 42

Malware

trojans, 5

viruses, 5

worms, 5

Quarantine

sending a file for expertise, 47

Technical support, 13

Technical Support Service, 57

APPENDIX F. LICENSE AGREEMENT

Standard End User Licence Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT") FOR THE LICENCE OF SPECIFIED SOFTWARE ("SOFTWARE") PRODUCED BY KASPERSKY LABS. ("KASPERSKY LABS").

IF YOU HAVE PURCHASED THIS SOFTWARE VIA THE INTERNET BY CLICKING THE ACCEPT BUTTON, YOU (EITHER AN INDIVIDUAL OR A SINGLE LEGAL ENTITY) CONSENT TO BE BOUND BY AND BECOME PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT, AND DO NOT INSTALL THE SOFTWARE.

IF YOU HAVE PURCHASED THIS SOFTWARE ON A PHYSICAL MEDIUM, HAVING BROKEN THE CD SLEEVE, YOU (EITHER AN INDIVIDUAL OR A SINGLE LEGAL ENTITY) HAVE CONSENTED TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT BREAK THE CD SLEEVE, DOWNLOAD, INSTALL, OR USE THIS SOFTWARE. YOU MAY RETURN THIS SOFTWARE FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM AN AUTHORISED KASPERSKY LABS DISTRIBUTOR OR RESELLER. THE RIGHT TO RETURN AND REFUND EXTENDS ONLY TO THE ORIGINAL PURCHASER.

All references to "Software" herein shall be deemed to include the software activation key ("Key Identification File") with which you will be provided by Kaspersky Lab as part of the Software.

1. Licence Grant. Subject to the payment of the applicable licence fees, and subject to the terms and conditions of this Agreement, Kaspersky Lab hereby grants you the non-exclusive, non-transferable right to use one copy of the specified version of the Software and the accompanying documentation (the "Documentation") for the term of this Agreement solely for your own internal business purposes. You may install one copy of the Software on one computer, workstation, personal digital assistant, or other electronic device for which the Software was designed (each a "Client Device"). If the Software is licensed as a suite or bundle with more than one specified Software product, this licence applies to all such specified Software products, subject to any restrictions or

usage terms specified on the applicable price list or product packaging that apply to any such Software products individually.

1.1 Use. The Software is licensed as a single product; it may not be used on more than one Client Device or by more than one user at a time, except as set forth in this Section.

1.1.1 The Software is "in use" on a Client Device when it is loaded into the temporary memory (i.e., random-access memory or RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that Client Device. This licence authorizes you to make only as many back-up copies of the Software as are necessary for its lawful use and solely for back-up purposes, provided that all such copies contain all of the Software's proprietary notices. You shall maintain records of the number and location of all copies of the Software and Documentation and will take all reasonable precautions to protect the Software from unauthorised copying or use.

1.1.2 If you sell the Client Device on which the Software is installed, you will ensure that all copies of the Software have been previously deleted.

1.1.3 You shall not decompile, reverse engineer, disassemble or otherwise reduce any part of this Software to a humanly readable form nor permit any third party to do so. The interface information necessary to achieve interoperability of the Software with independently created computer programs will be provided by Kaspersky Lab by request on payment of its reasonable costs and expenses for procuring and supplying such information. In the event that Kaspersky Lab notifies you that it does not intend to make such information available for any reason, including (without limitation) costs, you shall be permitted to take such steps to achieve interoperability, provided that you only reverse engineer or decompile the Software to the extent permitted by law.

1.1.4 You shall not make error corrections to, or otherwise modify, adapt, or translate the Software, nor create derivative works of the Software, nor permit any third party to copy the Software (other than as expressly permitted herein).

1.1.5 You shall not rent, lease or lend the Software to any other person, nor transfer or sub-licence your licence rights to any other person.

1.1.6 You shall not use this Software in automatic, semi-automatic or manual tools designed to create virus signatures, virus detection routines, any other data or code for detecting malicious code or data.

1.2 Server-Mode Use. You may use the Software on a Client Device or on a server ("Server") within a multi-user or networked environment ("Server-Mode") only if such use is permitted in the applicable price list or product packaging for the Software. A separate licence is required for each Client Device or "seat" that may connect to the Server at any time, regardless of whether such licenced Client Devices or seats are concurrently connected to or actually accessing or using the Software. Use of software or hardware that reduces the number of Client Devices or seats directly accessing or utilizing the Software (e.g.,

"multiplexing" or "pooling" software or hardware) does not reduce the number of licences required (i.e., the required number of licences would equal the number of distinct inputs to the multiplexing or pooling software or hardware "front end"). If the number of Client Devices or seats that can connect to the Software exceeds the number of licences you have obtained, then you must have a reasonable mechanism in place to ensure that your use of the Software does not exceed the use limits specified for the licence you have obtained. This licence authorises you to make or download such copies of the Documentation for each Client Device or seat that is licensed as are necessary for its lawful use, provided that each such copy contains all of the Documentation's proprietary notices.

1.3 Volume Licences. If the Software is licensed with volume licence terms specified in the applicable product invoicing or packaging for the Software, you may make, use or install as many additional copies of the Software on the number of Client Devices as the volume licence terms specify. You must have reasonable mechanisms in place to ensure that the number of Client Devices on which the Software has been installed does not exceed the number of licences you have obtained. This licence authorizes you to make or download one copy of the Documentation for each additional copy authorized by the volume licence, provided that each such copy contains all of the Document's proprietary notices.

2. Duration. This Agreement is effective for one (1) year unless and until earlier terminated as set forth herein. This Agreement will terminate automatically if you fail to comply with any of the conditions, limitations or other requirements described herein. Upon any termination or expiration of this Agreement, you must immediately destroy all copies of the Software and the Documentation. You may terminate this Agreement at any point by destroying all copies of the Software and the Documentation.

3. Support.

(i) Kaspersky Lab will provide you with the support services ("Support Services") as defined below for a period of one year following:

(a) Payment of its then current support charge, and:

(b) Successful completion of the Support Services Subscription Form as provided to you with this Agreement or as available on the Kaspersky Lab website, which will require you to produce the Key Identification File which will have been provided to you by Kaspersky Lab with this Agreement. It shall be at the absolute discretion of Kaspersky Lab whether or not you have satisfied this condition for the provision of Support Services.

(ii) Support Services will terminate unless renewed annually by payment of the then-current annual support charge and by successful completion of the Support Services Subscription Form again.

(iii) By completion of the Support Services Subscription Form you consent to the terms of the Kaspersky Lab Privacy Policy, which is attached to this Agreement,

and you explicitly consent to the transfer of data to other countries outside your own as set out in the Privacy Policy.

(iv) "Support Services" means

(a) Daily updates of the anti-virus database;

(b) Free software updates, including version upgrades;

(c) Extended technical support via e-mail and phone hotline provided by Vendor and/or Reseller;

(d) Virus detection and disinfection updates 24 hours per day.

4. Ownership Rights. The Software is protected by copyright laws. Kaspersky Lab and its suppliers own and retain all rights, titles and interests in and to the Software, including all copyrights, patents, trademarks and other intellectual property rights therein. Your possession, installation, or use of the Software does not transfer any title to the intellectual property in the Software to you, and you will not acquire any rights to the Software except as expressly set forth in this Agreement.

5. Confidentiality. You agree that the Software and the Documentation, including the specific design and structure of individual programs and the Key Identification File, constitute confidential proprietary information of Kaspersky Lab. You shall not disclose, provide, or otherwise make available such confidential information in any form to any third party without the prior written consent of Kaspersky Lab. You shall implement reasonable security measures to protect such confidential information, but without limitation to the foregoing shall use best endeavours to maintain the security of the Key Identification File.

6. Limited Warranty

(i) Kaspersky Lab warrants that for 90 days from first download or installation the Software will perform substantially in accordance with the functionality described in the Documentation when operated properly and in the manner specified in the Documentation.

(ii) You accept all responsibility for the selection of this Software to meet your requirements. Kaspersky Lab does not warrant that the Software and/or the Documentation will be suitable for such requirements nor that any use will be uninterrupted or error free;

(iii) Kaspersky Lab does not warrant that this Software identifies all known viruses, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus;

(iv) Your sole remedy and the entire liability of Kaspersky Lab for breach of the warranty at paragraph (i) will be at Kaspersky Lab option, to repair, replace or refund of the Software if reported to Kaspersky Lab or its designee during the

warranty period. You shall provide all information as may be reasonably necessary to assist the Supplier in resolving the defective item;

(v) The warranty in (i) shall not apply if you (a) make or cause to be made any modifications to this Software without the consent of Kaspersky Lab, (b) use the Software in a manner for which it was not intended or (c) use the Software other than as permitted under this Agreement;

(vi) The warranties and conditions stated in this Agreement are in lieu of all other conditions, warranties or other terms concerning the supply or purported supply of, failure to supply or delay in supplying the Software or the Documentation which might but for this paragraph (v) have effect between the Kaspersky Lab and you or would otherwise be implied into or incorporated into this Agreement or any collateral contract, whether by statute, common law or otherwise, all of which are hereby excluded (including, without limitation, the implied conditions, warranties or other terms as to satisfactory quality, fitness for purpose or as to the use of reasonable skill and care).

7. Liability

(i) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for (i) the tort of deceit, (ii) death or personal injury caused by its breach of a common law duty of care or any negligent breach of a term of this Agreement, (iii) any breach of the obligations implied by s.12 Sale of Goods Act 1979 or s.2 Supply of Goods and Services Act 1982 or (iv) any liability which cannot be excluded by law.

(ii) Subject to paragraph (i), the Supplier shall bear no liability (whether in contract, tort, restitution or otherwise) for any of the following losses or damage (whether such losses or damage were foreseen, foreseeable, known or otherwise):

(a) Loss of revenue;

(b) Loss of actual or anticipated profits (including for loss of profits on contracts);

(c) Loss of the use of money;

(d) Loss of anticipated savings;

(e) Loss of business;

(f) Loss of opportunity;

(g) Loss of goodwill;

(h) Loss of reputation;

(i) Loss of, damage to or corruption of data, or:

(j) Any indirect or consequential loss or damage howsoever caused (including, for the avoidance of doubt, where such loss or damage is of the type specified in paragraph (ii), (a) to (ii), (i).

(iii) Subject to paragraph (i), the liability of Kaspersky Lab (whether in contract, tort, restitution or otherwise) arising out of or in connection with the supply of the Software shall in no circumstances exceed a sum equal to the amount equally paid by you for the Software.

8. The construction and interpretation of this Agreement shall be governed in accordance with the laws of England and Wales. The parties hereby submit to the jurisdiction of the courts of England and Wales save that Kaspersky Lab as claimant shall be entitled to initiate proceedings in any court of competent jurisdiction.

9. (i) This Agreement contains the entire understanding between the parties with respect to the subject matter hereof and supersedes all and any prior understandings, undertakings and promises between you and Kaspersky Lab, whether oral or in writing, which have been given or may be implied from anything written or said in negotiations between us or our representatives prior to this Agreement and all prior agreements between the parties relating to the matters aforesaid shall cease to have effect as from the Effective Date. Save as provided in paragraphs (ii) - (iii), you shall not have any remedy in respect of an untrue statement made to you upon which you relied in entering into this Agreement ("Misrepresentation") and Kaspersky Lab shall not have any liability to the other than pursuant to the express terms of this Agreement.

(ii) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for any Misrepresentation made thereby if aware that it was untrue.

(iii) The liability of Kaspersky Lab for Misrepresentation as a fundamental matter, including a matter fundamental to the maker's ability to perform its obligations under this Agreement, shall be subject to the limitation of liability set out in paragraph 7(iii).